

**Partial English Translation of**  
**LAID OPEN unexamined**  
**JAPANESE PATENT APPLICATION**

**Publication No. 2001-024876**

[0072] to [0073]

[0072] Next, a case where “VC” is to be replaced thereby will be considered (Method 2).

[0073] Herein, the effective coefficient is expressed by the smallest bit number, as described above. Hence, no zero run length is involved as in the case of “VC”. Regarding the code replacement, any method can be employed if the bit number does not change. The reason for this is that no change occurs in the group number in the change in which no change occurs in the bit number, whereby appropriate decoding is enabled. Regarding the actual replacement, it can be considered to replace the bit at a place where the code in question is positioned by the bit of an embedded raw image. Herein, the bit position can be selected according to the random number.

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-024876

(43)Date of publication of application : 26.01.2001

(51)Int.Cl.

H04N 1/387

G06F 12/14

G06T 1/00

(21)Application number : 11-193332

(71)Applicant : CANON INC

(22)Date of filing : 07.07.1999

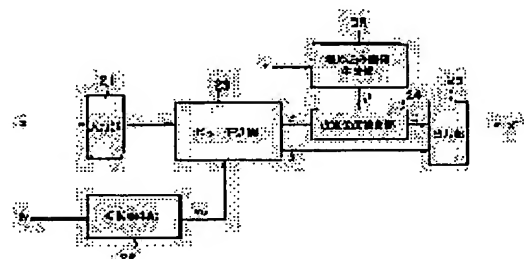
(72)Inventor : HAYASHI JUNICHI  
WAKAO SATOSHI

## (54) METHOD AND DEVICE FOR IMAGE PROCESSING AND STORAGE MEDIUM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To detect an alteration position when the alteration is performed by inputting image position information for instructing an image position at which another data are embedded in image data, generating sub-key information at a random number based on main key information and changing pixel data of the image position of the image data decided based on the image position information based on the sub-key information.

**SOLUTION:** In an extracting device of an electronic watermark, data to be inputted to an input part 21 are embedded image data (x') of the electronic watermark outputted from an electronic watermark embedding device and are inputted to a bit extractor 23. Also, a random number initial value Iv to be inputted to a random number generation part 22 is an initial value to the random number generation part 22, that is, main key information. The random number generator 22 to which the random number initial value Iv (the main key information) is inputted generates a random number progression (sub-key information) Rn and the generated random number progression Rn is inputted to the bit extractor 23. In the bit extractor 23, bit information is extracted from the embedded image data (x') by using this random number progression Rn.



## LEGAL STATUS

[Date of request for examination]

06.10.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-24876

(P2001-24876A)

(43) 公開日 平成13年1月26日 (2001.1.26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-リ-ト* (参考)
H 0 4 N 1/387		H 0 4 N 1/387	5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 5 7
G 0 6 T 1/00		15/66	B 5 C 0 7 6

審査請求 未請求 請求項の数26 O L (全 16 頁)

(21) 出願番号 特願平11-193332

(22) 出願日 平成11年7月7日 (1999.7.7)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 林 淳一

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(72) 発明者 若尾 聡

東京都大田区下丸子3丁目30番2号 キヤ  
ノン株式会社内

(74) 代理人 100076428

弁理士 大塚 康徳 (外2名)

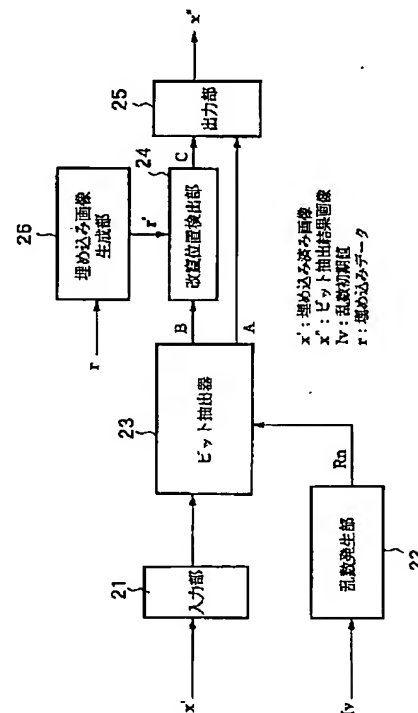
最終頁に続く

(54) 【発明の名称】 画像処理方法及び装置と記憶媒体

(57) 【要約】

【課題】 データに対して人為的な改竄がなされた場合に、その改竄位置を確実に検出する。

【解決手段】 画像データに別のデータを埋め込む画像位置を指示する埋め込みデータ  $r$  を入力し、その埋め込みデータ  $r$  に基づいて決定される画像データの画素データを、主鍵情報  $I_v$  に基づいて乱数的に生成された副鍵情報  $R_n$  に基づいて変更した埋め込み済み画像データ  $x'$  を生成する。この埋め込み済み画像データ  $x'$  を入力し、主鍵情報  $I_v$  に基づいて乱数的に生成された副鍵情報  $R_n$  に基づいて、そのデータ  $x'$  からビット情報を抽出し、そのビット情報の位置が埋め込みデータ  $r$  によって指示された位置に等しいかどうかによって、その埋め込み済み画像データ  $x'$  の改竄された位置を知ることができる。



## 【特許請求の範囲】

【請求項 1】 画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力手段と、主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成手段と、

前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更手段と、を有することを特徴とする画像処理装置。

【請求項 2】 画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力手段と、

前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成手段と、

前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出手段と、

前記抽出手段により抽出された前記画素データと前記鍵情報生成手段により生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較手段とを有し、

前記比較手段による比較結果に応じて前記埋め込み済み画像データの改竄位置を検出することを特徴とする画像処理装置。

【請求項 3】 前記画像データは多値画像データであって、前記副鍵情報は前記多値画像データの画素データのビット位置を指示する情報であることを特徴とする請求項 1 又は 2 に記載の画像処理装置。

【請求項 4】 前記画像データは符号化データであり、前記符号化データを解析する解析手段と、前記解析手段による解析に基づいて前記符号化データの符号を置き換える置換手段と、を更に有することを特徴とする請求項 1 に記載の画像処理装置。

【請求項 5】 前記符号化データが、入力系列において非零の係数から次の非零の係数までの係数の個数と、前記次の非零の係数の値の組合せをハフマン符号化した符号化データである場合、

前記置換手段は、前記非零の係数から次の係数までの係数の個数に対応するハフマン符号を前記非零の係数から前記次の非零の係数までの個数が増加しないように置き換えることを特徴とする請求項 4 に記載の画像処理装置。

【請求項 6】 前記符号化データが、入力系列において非零の係数から次の非零の係数までの係数の個数と、前記次の非零の係数の値の組合せをハフマン符号化した符号化データである場合、

前記置換手段は、前記次の係数の値に対応するハフマン符号を置き換えることを特徴とする請求項 4 に記載の画像処理装置。

【請求項 7】 前記別のデータが電子透かしを含むことを特徴とする請求項 1 に記載の画像処理装置。

【請求項 8】 埋め込みデータに従って入力画像データの位置を特定する位置特定手段と、

主鍵情報から副鍵情報を乱数的に生成する鍵情報生成手段と、

前記位置特定手段により特定された位置の画素情報を前記副鍵情報に基づいて別のデータに置き換える置換手段と、

10 前記置換手段により前記別のデータに置き換えられたデータに対して演算を行う演算手段と、

前記別のデータに置き換えられたデータと前記演算手段による演算結果とを合成して出力する合成手段と、を有することを特徴とする画像処理装置。

【請求項 9】 埋め込みデータに従って入力画像データの位置を特定された位置の画素情報を、主鍵情報から乱数的に生成された副鍵情報に基づいて別のデータに置き換え、前記別のデータに置き換えられたデータに対して実行された演算の結果とを合成して得られたデータを入力する入力手段と、

20 前記入力手段により入力されたデータを解析して前記データと前記演算の結果を抽出する解析手段と、

前記解析手段により抽出された前記データを演算する演算手段と、

前記解析手段により抽出された前記演算の結果と前記演算手段による演算結果とを比較する比較手段と、を有することを特徴とする画像処理装置。

【請求項 10】 前記入力画像データは符号化データであり、

30 前記符号化データを解析する解析手段と、前記符号化データの符号の位置を乱数的に選択し、前記選択された符号の位置のビットを抽出する手段を更に有することを特徴とする請求項 8 に記載の画像処理装置。

【請求項 11】 前記演算手段による演算はハッシュ値を算出する演算であることを特徴とする請求項 8 又は 9 に記載の画像処理装置。

【請求項 12】 画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力工程と、主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成工程と、

40 前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更工程と、を有することを特徴とする画像処理方法。

【請求項 13】 画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力工程と、

前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成工程と、  
前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出工程と、  
前記抽出工程で抽出された前記画素データと前記鍵情報生成工程で生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較工程とを有し、  
前記比較工程による比較結果に応じて前記埋め込み済み画像データの改竄位置を検出することを特徴とする画像処理方法。

【請求項 14】 前記画像データは多値画像データであって、前記副鍵情報は前記多値画像データの画素データのビット位置を指示する情報であることを特徴とする請求項 12 又は 13 に記載の画像処理方法。

【請求項 15】 前記画像データは符号化データであり、前記符号化データを解析する解析工程と、前記解析工程における解析に基づいて前記符号化データの符号を置き換える置換工程と、を更に有することを特徴とする請求項 12 に記載の画像処理方法。

【請求項 16】 前記符号化データが、入力系列において非零の係数から次の非零の係数までの係数の個数と、前記次の非零の係数の値の組合せをハフマン符号化した符号化データである場合、  
前記置換工程では、前記非零の係数から次の係数までの係数の個数に対応するハフマン符号を前記非零の係数から前記次の非零の係数までの個数が変化しないように置き換えることを特徴とする請求項 15 に記載の画像処理方法。

【請求項 17】 前記符号化データが、入力系列において非零の係数から次の非零の係数までの係数の個数と、前記次の非零の係数の値の組合せをハフマン符号化した符号化データである場合、  
前記置換工程では、前記次の係数の値に対応するハフマン符号を置き換えることを特徴とする請求項 15 に記載の画像処理方法。

【請求項 18】 前記別のデータが電子透かしを含むことを特徴とする請求項 12 に記載の画像処理方法。

【請求項 19】 埋め込みデータに従って入力画像データの位置を特定する位置特定工程と、  
主鍵情報から副鍵情報を乱数的に生成する鍵情報生成工程と、  
前記位置特定工程で特定された位置の画素情報を前記副鍵情報に基づいて別のデータに置き換える置換工程と、  
前記置換工程で前記別のデータに置き換えられたデータに対して演算を行う演算工程と、  
前記別のデータに置き換えられたデータと前記演算手段による演算結果とを合成して出力する合成工程と、を有することを特徴とする画像処理方法。

【請求項 20】 埋め込みデータに従って入力画像データの位置を特定された位置の画素情報を、主鍵情報から

乱数的に生成された副鍵情報に基づいて別のデータに置き換え、前記別のデータに置き換えられたデータに対して実行された演算の結果とを合成して得られたデータを入力する入力工程と、

前記入力工程で入力されたデータを解析して前記データと前記演算の結果を抽出する解析工程と、

前記解析工程で抽出された前記データを演算する演算工程と、

10 前記解析工程で抽出された前記演算の結果と前記演算工程による演算結果とを比較する比較工程と、を有することを特徴とする画像処理方法。

【請求項 21】 前記入力画像データは符号化データであり、

前記符号化データを解析する解析工程と、

前記符号化データの符号の位置を乱数的に選択し、前記選択された符号の位置のビットを抽出する工程を更に有することを特徴とする請求項 19 に記載の画像処理方法。

【請求項 22】 前記演算工程における演算はハッシュ値を算出する演算であることを特徴とする請求項 19 又は 20 に記載の画像処理方法。

【請求項 23】 コンピュータにより読取り可能な記憶媒体であって、

画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力工程モジュールと、

主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成工程モジュールと、

前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更工程モジュールと、を有することを特徴とする記憶媒体。

【請求項 24】 画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力工程モジュールと、

前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成工程モジュールと、

前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出工程モジュールと、

前記抽出工程で抽出された前記画素データと前記鍵情報生成工程で生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較工程モジュールとを有することを特徴とする記憶媒体。

【請求項 25】 埋め込みデータに従って入力画像データの位置を特定する位置特定工程モジュールと、  
主鍵情報から副鍵情報を乱数的に生成する鍵情報生成工程モジュールと、

前記位置特定工程で特定された位置の画素情報を前記副

鍵情報に基づいて別のデータに置き換える置換工程モジュールと、  
前記置換工程で前記別のデータに置き換えられたデータに対して演算を行う演算工程モジュールと、  
前記別のデータに置き換えられたデータと前記演算手段による演算結果とを合成して出力する合成工程モジュールと、を有することを特徴とする記憶媒体。

【請求項26】 埋め込みデータに従って入力画像データの位置を特定された位置の画素情報を、主鍵情報から乱数的に生成された副鍵情報に基づいて別のデータに置き換え、前記別のデータに置き換えられたデータに対して実行された演算の結果とを合成して得られたデータを入力する入力工程モジュールと、  
前記入力工程で入力されたデータを解析して前記データと前記演算の結果を抽出する解析工程モジュールと、  
前記解析工程で抽出された前記データを演算する演算工程モジュールと、  
前記解析工程で抽出された前記演算の結果と前記演算工程による演算結果とを比較する比較工程モジュールと、を有することを特徴とする記憶媒体。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、原画像データに電子透かしを埋め込んだ画像データを生成し、及び或はその画像データの改竄された箇所を特定する画像処理方法及び装置と記憶媒体に関するものである。

##### 【0002】

【従来の技術】近年のコンピュータ及びネットワークの発達は著しく、文字データ、画像データ、音声データ等、多種の情報がデジタル化され、コンピュータやネットワークを介して扱われるようになってきている。このようなデータはデジタルデータであるために、データの複製が容易にできる環境にある。このため、こうしたデータの著作権を保護するために、デジタル画像データやデジタル音声データの中に著作権情報や利用者情報を電子透かしとして埋め込む処理がなされる場合が多い。

【0003】この電子透かしとは、デジタル画像データや音声データに所定の処理を施すことによって、これらのデータに密かに情報を埋め込む技術である。この電子透かしをデータから抽出することにより、著作権情報や利用者情報を得ることができ、不正コピーを追跡することが可能である。

【0004】このような電子透かしを埋め込む方法には、空間領域に埋め込む方式と周波数領域に埋め込む方法の二つに分類できる。このうち、空間領域に埋め込む方式の例としては、パッチワークによるものとしてIBMの方式(W. Bender, D. Gruhl, N. Morimoto, Techniques for Data Hiding, "Proceedings of the SPIE", San Jose CA, USA, February 1995)などが挙げられる。また周波数領域に埋め込む方式の例としては、離散コサイン変換を利

用するものとしてNTT方式(中村, 小川, 高嶋等による“デジタル画像の著作権保護のための周波数領域における電子透かし方式”, SCIS' 97-26A, 1997年1月)の他に、離散フーリエ変換を利用するものとして防衛大の方式(大西, 岡, 松井, “PN系列による画像への透かし署名法”, SCIS' 97-26B, 1997年1月)や、離散ウェーブレット変換を利用するものとして三菱, 九大の方式(石塚, 坂井, 櫻井, “ウェーブレット変換を用いた電子透かし技術の安全性と信頼性に関する実験的考察”, SCIS' 97-26D, 1997年1月)及び松下方式(“ウェーブレット変換に基づくデジタル・ウォーターマーク画像圧縮, 変換処理に対するロバスト性について”, 井上, 宮崎, 山本, 桂, SCIS, 98-3. 2. A, 1998年1月)などが挙げられる。

【0005】このような電子透かしは、「攻撃」に対して耐性があることが必要である。ここで、電子透かしに対する「攻撃」について簡単に説明する。この「攻撃」とは、透かし情報を消去、或は破壊しようとする行為であり、2通りが考えられる。一つ目は画像処理によるものであり、透かし情報を埋め込んだ画像データに対して、画像圧縮、拡大及び縮小、切り取り、階調変換、プリントアウト及びスキニングなどの画像処理を施すものを含む。二つ目は人為的なものであり、透かし情報を埋め込んだ画像データに対してノイズを付加することや、透かし情報が埋め込んだと考えられる画像領域を削除することなどを含む。従って、このような攻撃のいずれに対しても、透かし情報は耐性を持つ必要がある。

【0006】ここで「耐性」とは、埋め込んだ情報が攻撃されても、その埋め込んだ情報を正確に取り出せることが可能であることを意味している。

【0007】しかしながら、あるアプリケーションでは、画像が攻撃された場合には、埋め込んだ情報を抽出する必要はなく、その代わりに、攻撃された場所などを特定する機能を有することを必要とする場合も考えられる。以下では、この機能のことを「改竄位置検出機能」と呼ぶことにする。

【0008】従来の、改竄位置検出機能を有する電子透かし方式としては、原画像が1画素当たり複数のビットから構成されるデータである場合には、複数のビットのうちLSB(Least Significant Bit)のビットを置き換えることにより透かし情報の埋め込みを行い、それを抽出する際には、LSBのビットだけ読み出すことにより抽出を行っていた。ここで、LSBとは1画素を構成する複数ビットの情報においてビット位置0(最小位)に位置するビット情報のことで、ビット位置とは、画素を構成するビット系列の中で、そのビットの存在する位置を示すものである。例えば、 $2^0=1$ を表すビットの存在する位置を表す場合、「ビット位置0」と呼び、 $2^1$

10

20

30

40

50

=2 (0は0乗を、1は1乗を示す)を表すビットの存在する位置を表す場合、「ビット位置1」と呼ぶ。ここで、ビット位置0をLSBと呼ぶのと同様に、1バイトデータにおけるビット位置7をMSB(Most Significant Bit)と呼ぶことにする。これ以降、「ビット位置」という表現は上述の定義に従うものとする。

【0009】このようなLSBへの透かし情報の埋め込みによって、画像処理手段を用いた攻撃に対しては、その改竄位置を特定することか可能であった。これは、LSBが画素を構成するビットのうち最小の大きさを表現しているものであるために、改竄された場合にはLSBのビットは変化しやすく、即ち変化した箇所を改竄された箇所として特定できるからである。ここで正しく抽出できない場合、LSBが“1”である確率と“0”である確率とが等しくなり、即ち、ランダムに“1”と“0”が出現することが予想される。よって、抽出の結果、ランダムに“1”と“0”が出現している領域を改竄された箇所であると検証することが可能となる。

【0010】しかしながら、以上のような方式は人為的な攻撃には弱かった。これは、LSBに固定されて埋め込まれているために、全ての画素のLSBを抽出するといった探索により、電子透かしが埋め込まれたことが第三者に容易に類推されることが考えられる。従って、もし画像データに電子透かしが埋め込まれていることが第三者に知られた場合には、その第三者は透かしが埋め込まれているLSBの状態をそのままにして、それ以外のビット位置のデータを変更することにより、容易に画像データを容易に改竄することができる。具体例として、画像の内容を改竄する前にLSBの情報を保存しておき、その後、その画像の内容を改竄し、こうして改竄した画像データのLSBだけを予め保存していた情報に置き換えるといった人為的な手段によって、その改竄した画像位置を特定できないようにすることが考えられる。

#### 【0011】

【発明が解決しようとする課題】以上述べたように従来の技術によれば、透かし情報を埋め込んだ画像に対して改竄を施した場合、その改竄された画像位置を確実に特定することができなかった。

【0012】本発明は上記従来例に鑑みてなされたもので、データに対して人為的な改竄がなされた場合に、その改竄位置を確実に検出できる画像処理方法及び装置を提供することを目的とする。

【0013】また本発明の目的は、入力された原画像データの画素位置を指示し、主鍵情報に基づいて、その指示された画素位置の特定の部分を書き換えることにより、入力した画像データに所定のデータを埋め込むことができる画像処理方法及び装置を提供することにある。

【0014】また本発明の目的は、このような所定のデータが埋め込まれたデータに対してなされた改竄処理を検知し、その改竄位置をも検知できるようにした画像処

理方法及び装置を提供することにある。

#### 【0015】

【課題を解決するための手段】上記目的を達成するために本発明の画像処理装置は以下のような構成を備える。即ち、画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力手段と、主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成手段と、前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更手段と、を有することを特徴とする。

【0016】また本発明の画像処理装置は、画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力手段と、前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成手段と、前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出手段と、前記抽出手段により抽出された前記画素データと前記鍵情報生成手段により生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較手段とを有し、前記比較手段による比較結果に応じて前記埋め込み済み画像データの改竄位置を検出することを特徴とする。

【0017】上記目的を達成するために本発明の画像処理方法は以下のような工程を備える。即ち、画像データに別のデータを埋め込む画像位置を指示する画像位置情報を入力する入力工程と、主鍵情報に基づいて乱数的に副鍵情報を生成する乱数生成工程と、前記画像位置情報に基づいて決定される画像データの画像位置の画素データを前記副鍵情報に基づいて変更する画素変更工程と、を有することを特徴とする。

【0018】また本発明の画像処理方法によれば、画像データに別のデータを埋め込む画像位置を指示する画像位置情報に基づいて決定される画像データの画像位置の画素データを、主鍵情報に基づいて乱数的に生成された副鍵情報に基づいて変更することにより得られた埋め込み済み画像データを入力する入力工程と、前記主鍵情報を入力して前記副鍵情報を生成する鍵情報生成工程と、前記副鍵情報に基づいて前記埋め込み済み画像データの画素データを抽出する抽出工程と、前記抽出工程で抽出された前記画素データと前記鍵情報生成工程で生成された前記副鍵情報に基づく画素位置の画素データとを比較する比較工程とを有し、前記比較工程による比較結果に応じて前記埋め込み済み画像データの改竄位置を検出することを特徴とする。

#### 【0019】

【発明の実施の形態】以下、添付図面を参照して本発明の好適な実施の形態を詳細に説明する。

【0020】【実施の形態1】図1は、本発明の実施の

10

20

30

40

50

形態1に係る電子透かしの埋め込み装置の概略構成を示すブロック図である。

【0021】図1において、入力部11へ入力されるデータxは、1画素当たり所定のビット数を有する多値画像データである。以下では、このデータxを原画像データと呼ぶ。また入力部12へ入力されるデータrは、1画素を1ビットで表わす二値画像データで、以下では、このデータを埋め込みデータと呼ぶ。ここで、この埋め込みデータは、人間の視覚にとって意味のある内容であっても、或は人間の視覚にとって意味のない内容であっても良い。意味のある内容である場合には、例えば、著作者の持つロゴマークのようなものであってもよい。この場合は、このロゴマークが埋め込まれた画像から、その著作権情報を読み取ることも可能である。また一方、意味のない内容である場合には、IDの様なものを2進数で表現したものであっても良い。ここでIDとは固有の値を意味している。例えば、利用者IDの場合には、その利用者にとって固有の値を表し、デバイスIDの場合には、そのデバイスにとって固有の値を表している。この場合、このようなIDが埋め込まれた画像から、利用者情報、或は利用デバイス情報などを読み取ることも可能である。

【0022】また、乱数発生器13へ入力されるデータIvは、乱数発生器13への初期値、即ち主鍵情報を示している。また、入力部12へ入力された埋め込みデータrは、埋め込み画像生成器14へ入力される。この埋め込み画像生成器14の詳細な動作については後述する。こうして埋め込み画像生成器14からは、原画像データxと等しい面積の画像データが出力され、この画像データはビット置き換え器15へ入力される。また入力部11へ入力された原画像データxは、ビット置き換え器15へ入力される。このビット置き換え器15の詳細な動作についても後述する。こうして、このビット置き換え器15からは、原画像データxのうち埋め込みデータrにより指定された位置（例えば埋め込みデータr'の対応するビットが“1”）の画素情報の特定のビットだけが置き換えられた画像データが出力され、その画像データは出力部16を介して、埋め込み済み画像データx'として出力される。

【0023】次に、各部の動作の詳細について説明する。

【0024】まず、埋め込み画像生成器14の詳細な動作について解説する。

【0025】埋め込み画像生成器14は、入力された埋め込みデータrを基に、その埋め込みデータrを原画像データxの大きさに等しいサイズに変換する。以下では、この埋め込み画像生成器14から出力された画像データを埋め込み画像データr'と呼ぶことにする。この埋め込み画像生成器14におけるサイズ変換には、埋め込みデータrを繰り返し並べる方式、或は埋め込みデー

タrを原画像データxの大きさに拡大（変倍）処理する方式など、種々のものが考えられる。なお、この埋め込み画像生成器14から出力される埋め込み画像データr'も、1画素に付き1ビットのデータを有する2値データでなければならない。

【0026】次に、乱数発生器13の詳細な動作について解説する。

【0027】乱数発生器13には、乱数初期値Iv、即ち主鍵情報が入力される。本実施の形態1に係る処理を安全に用いるために、乱数初期値Ivを公開情報とする場合には、本実施の形態1で用いる乱数発生器13は、その乱数の発生方式が非公開のもの、或は別の非公開情報を用いるものでなければならない。その一方、乱数発生器14における乱数発生方式が公開されたものである場合には、乱数初期値Ivを非公開情報としなければならない。つまり、ビット置き換え器15へ入力される乱数系列、即ち副鍵情報Rnを非公開情報とする必要がある。これらのうち、いずれを公開情報とし、いずれを非公開情報とするかは、各アプリケーションに応じて決定することが可能である。

【0028】次に、ビット置き換え器15の詳細な動作について解説する。

【0029】このビット置き換え器15は、埋め込み画像データr'を原画像データxに埋め込む、所謂電子透かし埋め込み処理を行う部分である。このビット置き換え器15においては、埋め込み画像生成器14から出力された埋め込み画像データr'と、入力部11から出力された原画像データxの対応する画素位置（例えば埋め込みデータr'の対応するビットが“1”）において、その画素値である複数ビット（この実施の形態では8ビット）の内のあるビットの置き換え処理が施される。このビットの置き換え処理は、原画像データxの持つ輝度値データをビットプレーンに展開した領域に対して施される。いま例えば原画像データが256階調（8ビット）を持つ場合、これら8ビットのうちの1ビットが選択されて、このビットが埋め込み画像データr'の対応するビットで置き換えられる。この埋め込まれる（選択される）ビット位置は、乱数発生器13からの出力である副鍵情報Rnによって決定される。

【0030】例えば、原画像データxが1画素当たり8ビットの2進符号によって表現されている場合、乱数発生器13からは“0”から“7”の値を持つ乱数データ列Rnが出力される。この乱数データ列Rnの値に対応するビット位置が、前述したビット置き換えの対象となるビット位置を示している。

【0031】ここで、このビット置き換えの対象となるビット位置の選択には、注意が必要である。例えば、選択されるビット位置がMSBに近い値を持つような場合には、埋め込み済み画像データx'の画素値が原画像データxの対応する画素値から大きく異なり、これにより

埋め込み済み画像データ  $x'$  が、原画像データ  $x$  に比べて劣化することが予想される。これは、例えば 1 画素当たり 8 ビットで構成される画像データの場合に、MSB の値を変化させることにより、輝度値において 2 の 7 乗 = 128 の変化が生じることによる。また、LSB に限定したビット位置ばかりが選択されると、前述の従来の技術で述べたように、人為的な攻撃に対しては耐性が弱くなる。即ち、例えば、ビット置き換えの対象が LSB、即ちビット位置 0 だけに限定されているような場合には、置き換えられたビットは容易に書き換えられてしまうと考えられる。また或は、ビット置き換えの対象位置が、ビット位置 0 とビット位置 1 である場合には、ビット位置の書き換えには、 $(XS \times YS)$  の 2 乗の探索を必要とする。ここで、XS 及び YS は原画像データ  $x$  の横方向の大きさ及び縦方向の大きさを示している。

【0032】一般に、ビット置き換えの対象位置をビット位置 0 からビット位置  $n$  とした場合には、ビット位置の書き換えには、 $(XS \times YS)$  の  $n$  乗の探索を必要とする。従って、以上述べたような探索により、埋め込んだ情報（即ち、埋め込んだ全ての画素でのビット位置）が解ってしまった場合、画像の内容を変化させるような改竄が行われた後で、これらの埋め込んだ情報を元の埋め込んだ情報に置き換えることにより、後に述べるビット抽出器 23 において、改竄されていない画像であると偽ることが可能となってしまう。この点から、ビット置き換えの対象に選択するビット位置は LSB に近いビット位置が良いといえる。このように LSB に近いビットを選択して、埋め込みデータ  $r'$  を埋め込むことによって、原画像データ  $x$  からの視覚的な画質劣化を抑えて、且つ、画像処理による改竄をされた場合に、その改竄を検証し、更に改竄された位置を特定することが可能となる。即ち、画像が改竄されたにも関わらず、その改竄を検証できなかったり、改竄位置を特定できなくなることが防止できる。

【0033】以上述べたような処理によって、電子透かしの埋め込み処理を行うことにより、生成された埋め込み済み画像データ  $x'$  は出力部 16 を介して出力される。

【0034】図 2 は、本発明の実施の形態 1 に係る電子透かしの抽出装置の概略構成を示すブロック図である。

【0035】図 2 において、入力部 21 へ入力されるデータ  $x'$  は、前述の図 1 における電子透かし埋め込み装置から出力された電子透かしの埋め込み済み画像データ  $x'$  である。また乱数発生器 22 へ入力されるデータ  $I_v$  は、乱数発生器 22 への初期値、即ち主鍵情報である。主鍵情報  $I_v$  の値は、図 1 において乱数発生器 13 へ入力されるデータ  $I_v$  と完全に等しいものでなければならない。

【0036】入力部 21 に入力された埋め込み済み画像データ  $x'$  は、ビット抽出器 23 へ入力される。乱数初

期値  $I_v$ （主鍵情報）が入力された乱数発生器 22 は乱数列（副鍵情報） $R_n$  を生成し、その生成された乱数列  $R_n$  がビット抽出器 23 へ入力される。ビット抽出器 23 では、この乱数列  $R_n$  を用いて埋め込み済み画像データ  $x'$  からビット情報を抽出する。ここで、乱数発生器 22 から出力される乱数列  $R_n$  は、前述の図 1 における乱数発生器 13 と同じ構成であるため、ビット抽出器 23 が対象とするビット位置も、図 1 におけるビット置き換え器 15 が対象としたビット位置に一致している。よって、以上の処理によって抽出されるビット情報、即ちビット抽出結果を示す画像データ  $x''$  は、埋め込み済み画像データ  $x'$  が改竄されていない場合には、図 1 における、原画像データ  $x$  に等しいはずである。

【0037】一方で、埋め込み済み画像データ  $x'$  が改竄されている場合には、埋め込みデータ  $r$  とは、改竄されている位置に関して誤って検出される。ここで、埋め込み済み画像データ  $x'$  から検出されたビット抽出結果に対応する画像が正しいか、或は誤っているかの判断は、図 1 において埋め込みデータ  $r$  としてどのようなものが埋め込まれているかによって方法が違ふ。

【0038】例えば、埋め込みデータ  $r$  として、人間の視覚にとって意味のある内容のものが埋め込まれている場合には、図 2 における改竄位置検出器 24 を用いなくとも（経路 A）人間の視覚によって判断可能である。誤って検出される場合、どのような改竄が行われたかにもよるが、確率的には 2 進符号 “1” と “0” が等しい確率で出現することが予想される。即ち、改竄された箇所は、人間の目には、白色ノイズに近い性質を持つ画像として見えるはずである。

【0039】更に、図 2 において埋め込みデータ  $r$  が、ビット抽出器 23 へ入力可能である場合には、この埋め込みデータ  $r$  を改竄位置検出器 24 へ入力することにより、上述の判断は改竄位置検出器 24 により行うことが可能である。これは、図 2 において、改竄位置検出器 24 を通る経路、即ち B の経路を通る場合である。

【0040】ここで改竄位置検出器 24 には、埋め込みデータ  $r$ 、及び図 2 から出力されたビット抽出結果を示す画像データ (B) が入力される。埋め込みデータ  $r$  は、埋め込み画像生成器 26 で所定の処理が施された後に、改竄位置検出器 24 へ入力される。この画像生成器 26 で施される処理は、図 1 における埋め込み画像生成器 14 で行われた処理と同様の処理でなければならない。こうして改竄位置検出器 24 では、入力された 2 つの画像データの同じ座標位置においてビットを比較し、等しい場合に “1” を、等しくない場合には “0” を出力する。これにより、ビット抽出結果画像として改竄位置では “0” が、一方で改竄されていない位置では “1” が出力される。このビット抽出結果を示す画像データ  $c$  は、アプリケーションが改竄位置を特定するためにも用いることが可能であるし、更に、人間の目によ

10

20

30

40

50

て改竄位置を特定することも可能である。

【0041】尚、人間の目によって改竄位置を特定する場合には、前述の方式よりも、この方式のほうが正確に微小な改竄を検出することが可能である。

【0042】更に、埋め込みデータ  $r$  が白色単色である場合には、改竄が検出された画素に関しては黒色画素とすることにより、より分かりやすく改竄位置を表現することも可能である。

【0043】【実施の形態2】次に本発明の実施の形態2について説明する。この実施の形態2では、圧縮された画像データに対して前述の実施の形態1を適用するものである。前述の実施の形態1では、埋め込みの対象となる入力画像データは、1画素当たり所定のビット数（前述の例では8ビット）を持つ多値画像データであった。これに対し本実施の形態2では、埋め込みの対象となる入力画像データは、符号化された画像データである。なお、この符号化された画像データには、J P E G によって圧縮された画像データも含まれる。以下、本実施の形態2では、符号化データがJ P E G データである場合について説明する。

【0044】まず、J P E G 符号化について解説をする。

【0045】図3(a)は、J P E G の符号化手順例を説明するブロック図である。

【0046】まず、符号化する静止画の画像データを  $8 \times 8$  画素のブロックに分割し、各ブロック毎にD C T（離散的コサイン変換）を行う（画像変換器301）。以下、そのD C T (Discrete Cosine Transform) したブロックをD C T 係数ブロック、D C T 係数ブロックの1係数をD C T 係数、1枚の画像のD C T 係数ブロックの集合をD C T 係数ブロック群と呼ぶとする。

【0047】次に、D C T 係数ブロック群を任意の量子化テーブルを用いて、量子化器302により量子化を行う。以下、このD C T 係数ブロックを量子化したブロックを量子化D C T 係数ブロック、1枚の画像の量子化D C T 係数ブロックの集合を量子化D C T 係数ブロック群と呼ぶとする。

【0048】そして、量子化D C T 係数ブロック群をハフマン符号化する（エントロピー符号化器303）。このハフマン符号化したデータがJ P E G データになる。このとき用いるハフマンテーブルは、予め用意していたテーブルであっても、各画像毎に作成したテーブルであってもよい。

【0049】J P E G データは、このハフマン符号化したデータと、圧縮時に用いた量子化テーブルとハフマンテーブルを含む（後述：図4参照）。ここで、量子化D C T 係数ブロックは、各D C T 係数ブロックを各々量子化テーブルによって定められた値で除算することによって得られる。例えば、輝度成分に対する量子化テーブル、或は色差成分に対する量子化テーブルは、 $8 \times 8$  の

D C T 係数ブロックに対して、それぞれ図5(a)

(b) のように与えられる。

【0050】これらの量子化テーブルは低周波成分により多くのビットを割り当て、高周波成分にはより少ないビットを割り当てるようにして、人間の視覚特性を考慮して構成されている。よって、D C T 係数ブロックの値が「-36」である場合、量子化テーブル値が「18」であればその量子化D C T 係数ブロック値は「-2」であり、「99」であればその量子化D C T 係数ブロック値は「0」である。

【0051】また、ハフマン符号化は、量子化D C T 係数をD C 係数とA C 係数に分けて別々に行われる。D C 係数は1つ前のブロック群のD C 係数との差分をD C 用のテーブルを用いて符号化される。

【0052】A C 係数は図6のようなジグザグスキャン順に並び替えて、「0」の係数の連続長（ラン長）と、「0」以外の係数値を組み合わせたテーブルを用いて符号化される。

【0053】次に、このJ P E G データの例を図4に示す。

【0054】図4は、J P E G のシーケンシャル方式で圧縮したデータの構成例を示す図である。

【0055】このシーケンシャル方式とは、デコードを行うと上から順に鮮明な画像がでてくる方式で、これに対して、最初画像全体を不鮮明に表示し、徐々に鮮明になってくる方式はプログレッシブ方式と呼ばれている。このJ P E G データは、マーカと呼ばれるデータ内でユニークな2バイトのコードによってフォーマットされている。

【0056】まず最初の「S O I」マーカは、J P E G データのスタートを表わしている。次の「D Q T」マーカ部は、量子化テーブルの定義を表わしており、圧縮時に使用した量子化テーブルを「D Q T」マーカの後ろに格納している。次の「S O F O」マーカ部は、D C T を使ったシーケンシャル方式で圧縮した場合に、「S O F O」マーカを使用し、このマーカの後ろに、圧縮してある画像のサイズやサンプリング率、コンポーネント数、コンポーネント毎の量子化テーブルの識別子等の圧縮時のパラメータが格納される。次の「D H T」マーカ部は、ハフマンテーブルの定義を表わしており、この「D H T」マーカの後ろには、圧縮時に使用したハフマンテーブルが格納されている。次の「S O S」マーカ部は、実際に画像を符号化したハフマン符号を格納している。ここでのハフマン符号は、D C T 係数の直流成分、及び交流成分において異なる符号化が施されていることに注意する必要がある。

【0057】J P E G においては、D C T 係数のうちの直流成分は、隣り合うD C T ブロックの直流成分の差分値をハフマン符号で表現している。一方、交流成分では、差分値は用いず、ブロック内でジグザグスキャンさ

れたシーケンスの零ランレングスと有効係数との組合せをハフマン符号で表現している。このハフマン符号と、有効係数の大きさを最小のビット数で表現した符号の組合せが符号化データである。以降の説明では、前者に相当する符号を「GC」、後者に相当する符号を「VC」と定義する。ここで有効係数とは零でない係数である。

【0058】交流成分のハフマン符号化に関して例を挙げて説明する。

【0059】例えば、交流成分として直流成分のすぐ右に位置する値「-3」を持つ係数をハフマン符号化する場合を考える。この場合、図7に示すような表を用いて係数がグループ化される。即ち、例えば値「-3」の場合には、グループ番号として「2」が選択される。更に、零ランレングスは「0」である。これらグループ番号と零ランレングスの組合せ(0, 2)を基に、図8に示すハフマンテーブルを用いてハフマン符号化される。

【0060】この例の場合には、「GC」としてハフマン符号「01」が選択され記憶される。この後に、「VC」として「-3」を最小のビット数で表現した「00」が続いて記憶される。その結果として、この例における交流成分「-3」には、「0100」というハフマン符号が選択される。

【0061】そして「SOS」マーカの後に、コンポネント毎のハフマンテーブルへの識別子等の情報が入ったヘッダが数バイト続いた後、画像を符号化したハフマン符号が続く。そして最後に、「EOI」マーカにより符号化された画像データの終了が示されている。

【0062】この例ではマーカの順を図4のように示したが、実際のデータではこの順番である必要はないし、またマーカの数が2つ以上の場合もある。

【0063】図3(b)は、図3(a)の手順で圧縮したJPEGデータの復号化装置の構成例を示したブロック図である。

【0064】この復号化処理では、まずJPEGデータ内のハフマンテーブルを用いて、ハフマン符号のハフマン復号化を行って、量子化DCT係数ブロック群に復号する(エントロピー復号器304)。次に逆量子化器305を用いて、量子化DCT係数ブロック群を、JPEGデータの量子化テーブルを用いて逆量子化し、DCT係数ブロック群に復号する。そして次に画像逆変換器306により、そのブロック群をIDCT(Inverse DCT: 逆DCT)を行って、8×8画素のブロックに戻し、それを再構成する。このような手順によってJPEGデータから復号した画像データを得ることができる。

【0065】図9は、本発明の実施の形態2に係る電子透かし埋め込み装置の概略構成を示すブロック図である。

【0066】図9において、入力部901を介して入力される入力データ(Code)は、図4のようなデータ形式で構成されたJPEG符号化データである。また、乱数初

期値Iv、及び乱数発生器905は、前述の実施の形態1の乱数発生器13と同様のものを用いる。入力されたJPEG符号化データ(Code)は、解析器902において、JPEGの符号化フォーマットに従って解析される。ここで解析とは、入力されたビット系列が、JPEGの符号化フォーマットに従って、符号化データとして意味のあるデータとして理解されることである。このうち、電子透かしの埋め込みの対象となる交流成分のハフマン符号が、DCTブロック毎に置換器903に入力される。この置換器903は、DCTブロック毎に埋め込みデータのビット情報に応じたハフマン符号の置き換えを行う。ここで、ハフマン符号の置き換えの対象となる符号は、できる限りブロックの中で交流成分が望ましい。

【0067】これは置換器902に入力されたスキャンデータの中で、出来るだけ後ろに位置する符号を対象とすることを意味する。なぜなら、スキャンデータはDCTブロックの中でジグザグスキャンされているため、スキャンデータの中で後ろに位置するデータほど高域成分であるからである。

【0068】次に、選択された符号に対して置き換え処理を行う方式に関して説明する。

【0069】まず、「GC」が置き換えの対象となる場合を考える(方式1)。

【0070】これは前述したように、零ランレングスと有効係数の組合せによって表現されているものである。このため、ハフマン符号の置き換えの結果、零ランレングスの値が変化してしまうような場合には、復号時に正しい復号をすることができない。なぜなら、有効係数の位置を正しく決定することが出来ないからである。これを解決する一つの方式として、JPEG符号化の際に、図8に示すようなハフマンテーブルを用いているような場合には、この表の横方向の置き換えに限定することが考えられる。例えば、符号「00」を符号「01」に置き換えることなどが考えられる。更に、横方向の置き換えを行った後においては、その後に続く「VC」の変更が必要である。これは、符号「00」を符号「01」に置き換えることによって、零ランレングスは変わらないが、その一方で、グループ番号が変わるからである。これに関しては、置き換える前の符号の表現している値との差が最小になるような値を表現する符号を、置き換え後のグループから選択することによって解決可能である。

【0071】本実施の形態における横方向の置き換えに関しては、例えば、埋め込みデータのビット情報が“0”である場合には、最も近い奇数グループ番号へ、一方で埋め込みデータのビットが“1”である場合には、最も近い偶数グループ番号へ置き換えることが、画質劣化を最小に抑えるという観点から現実的である。

【0072】次に、「VC」が置き換えの対象となる場合を考える(方式2)。

10

20

30

40

50

【0073】これは前述したように、有効係数を最小のビット数で表現しているものである。よって「VC」の場合のように零ランレングスに関しては関連しない。この符号の置き換えに関しては、ビット数が変化しないような方法であれば、任意の方法が選択可能である。なぜなら、ビット数が変化しないような変化であれば、グループ番号は変わることがなく、即ち正しく復号可能であるからである。実際の置き換えに関しては、その符号のあるビット位置のビットを、埋め込み原画像のビットに置き換えることが考えられる。この時のビット位置は乱数によって選択可能である。

【0074】以上、述べた方式によってビット置き換えが行われ、出力部904を介して、JPEGデータが出力される。

【0075】図10は、本実施の形態2に係る電子透かしの抽出装置の概略構成を示すブロック図である。

【0076】図10において、入力部1001を介して入力される入力データxは、図9に示した電子透かし埋め込み装置により、電子透かしが埋め込まれたJPEG符号化データxである。また、乱数初期値Iv及び乱数発生器905に関しては、前述の実施の形態1で説明した乱数発生器13と同じものである。ここで、入力されたJPEG符号化データxは、解析器1002において、JPEGの符号化フォーマットに従って解析される。このうち、電子透かしが埋め込まれている交流成分のハフマン符号が、DCTブロック毎に抽出器1003に入力される。

【0077】この抽出器1003は、DCTブロック毎に符号化データxから電子透かしの抽出を行う。この抽出器1003は、乱数発生器905から得られる乱数列Rnによって、ブロック中において、どの符号化された係数に対して電子透かしが埋め込まれているかを特定する。次に、この特定された係数を表現している符号から、電子透かしの抽出を行う。

【0078】「VC」及び「GC」の両方が置き換えの対象となる場合を考える（方式1に対応）。

【0079】これは、前述したように、「VC」と「GC」の両方に対して、電子透かしの埋め込みが行われており、その符号が属するグループ番号の奇数/偶数によって、ビットを判定することが可能である。

【0080】入力されたJPEGデータの中で、「HDT」マーカの後に記憶されているハフマンテーブルを用いて、選択されたハフマン符号からグループ番号を求め、これが偶数であった場合ビット“1”を出力し、奇数であった場合ビット“0”を出力する。

【0081】次に、「VC」が置き換えの対象となる場合を考える（「方式2」に対応）。これは、選択された符号の中で、乱数Rnにより埋め込みビット位置を特定し、その特定されたビット位置のビット情報を出力することによって抽出可能である。以上の処理により、電子

透かしを抽出し、出力部1004を介して、ビット抽出結果を示す画像として出力される。

【0082】このビット抽出結果画像から、改竄されているかどうかを検証する方式に関しては、前述の実施の形態1で説明したのと同様の方法を用いることが可能である。

【0083】〔実施の形態3〕次に本発明の実施の形態3について説明する。この実施の形態3は実施の形態1或は実施の形態2を、ハッシュ値との組合せによって実現する方式である。

【0084】一般的に、このハッシュ値を用いることによりデジタルデータが改竄されているかどうかを検証することができる。

【0085】次に、このハッシュ値について解説する。

【0086】ハッシュ値hとは、ハッシュ関数 $f: x \rightarrow h$ により求められる長い入力例xの圧縮値である短い出力hである。また、ハッシュ関数fは一方方向性関数であり、 $r(x') = r(x)$ を満たす異なる入力x, x'を求めるのは難しいという性質をもつ。このハッシュ関数fの代表的なものとしては、MD5(Message Digest 5)、SHA(Secure Hash Algorithm)などがある。このハッシュ関数の詳細については、岡本英司著「暗号理論入門」（共立出版株式会社）に詳しい。

【0087】以上、述べたような性質を持つハッシュ値を用いて、デジタルデータの改竄検証を行うことが可能である。

【0088】これは、あるデジタルデータのハッシュ値hがわかっている場合に、そのデータが改竄されているかどうかを検証するためには、改めてデジタルデータのハッシュ値hを算出し、それとわかっているハッシュ値hと比較することによって実現可能である。即ち、改竄されていない場合は、これらは一致し、改竄されている場合にはこれらは一致しない。

【0089】以上述べた方式によって、デジタルデータが改竄されているかどうかを検証することが可能である。しかし、この方式に用いるデジタルデータとして画像データが用いられる場合、あるアプリケーションにおいては、改竄されていた場合には、画像データのどの箇所が改竄されているかを知りたい場合も考えられる。こうした場合、前述の方式では不十分である。なぜなら、ハッシュ値hを算出し、比較するといった前述の方式では、画像データの少なくとも1ビットが改竄されている場合には、ハッシュ値hが一致しないという比較結果は得られることができるが、その一方で「どの1ビットが改竄されたか」ということに関しては何ら情報を得る手段がない。

【0090】そこで、本実施の形態3においては、ハッシュ値hによる改竄検出と、前述の実施の形態1或は実施の形態2による改竄検出とを組み合わせる方式を提案する。

10

20

30

40

50

【0091】図11は、本発明の実施の形態3に係る電子透かしの埋め込み装置の構成を示すブロック図である。

【0092】本装置への入力は、原データとして、1画素当たり所定数のビットを有する多値画像データ或は符号化データx、及び埋め込みデータr、及び乱数初期値kである。ここで、入力データxが1画素当たり所定数のビットを持つ多値画像データの場合は、図11の電子透かし埋め込み器1101は、前述の実施の形態1で説明したような方式の装置を用いるべきであり、一方、入力データxが符号化データの場合には、図11の電子透かし埋め込み器1101は、前述の実施の形態2で説明した方式の装置を用いるべきである。

【0093】また、埋め込みデータr及び乱数初期値kは、前述の実施の形態1及び実施の形態2で述べたものと同様のものが考えられる。

【0094】以上述べた様な構成によって、入力されたデータxには、電子透かし埋め込み器1101によって埋め込みデータrが埋め込まれる。ここで、電子透かし埋め込み器1101から出力されるデータを埋め込み済みデータx1と呼ぶ。この埋め込み済みデータx1は、演算器1102及び合成器1103に入力される。演算器1102では、この埋め込み済みデータx1に対して前述したハッシュ演算などを施し、その演算結果であるハッシュ値hなどが出力される。また合成器1103には、電子透かし埋め込み器1101からの出力である埋め込み済みデータx1及び演算器1102からの出力である埋め込み済みデータx1のハッシュ値hが入力され、これらが合成される。この合成には、ハッシュ値hを、入力データxの形式に対応した付加的な情報が記述可能な箇所へ書き込むことなどが考えられる。例えば、入力データxがJPEG符号化データである場合には、その埋め込み済みデータx1もJPEG符号化データとなる。この場合には、JPG符号において、COMがコメントのためのマークとして定義されているために、M\_COMの後にハッシュ値hを記述することが可能である。

【0095】また同様に、入力データxが1画素当たり所定数のビットを持つ多値画像データである場合にも、それが用いている画像フォーマットにおいて、付加的な情報を記述可能な箇所へ書き込むことが考えられる。例えば、入力データxがPBMフォーマットである場合、記号「#」の後に続く改行コードまでのデータは、コメントであるとみなされるため、この領域にハッシュ値hを記載することができる。

【0096】更に、入力データxがFlashPixファイル・フォーマットの場合では、ハッシュ値hを属性情報としてプロパティセットの中に格納しておくこともできる。

【0097】以上のように、合成器1103からはハッシュ値hと埋め込み済みデータx1とが合成されたデー

タx'が出力される。

【0098】以下では、この合成器1103からの出力をハッシュ値hを含む埋め込み済みデータx'と呼ぶ。

【0099】次に図12は、本実施の形態3に係る改竄検出装置の構成を示すブロック図である。

【0100】本装置への入力は、図11に示した電子透かし埋め込み装置から出力されたハッシュ値hを含む埋め込み済みデータx'及び乱数初期値kである。この乱数初期値kは、図11に示す装置において入力されたものと等しい値である場合、正常に電子透かしの抽出することが可能である。この入力されたハッシュ値hを含む埋め込み済みデータx'は解析器1201へ入力される。この解析器1201では、入力された画像フォーマットに応じた解析が行われ、ハッシュ値hと埋め込み済みデータx1を出力する。このうち埋め込み済みデータx1は、演算器1202及び切替え器1204に入力される。演算器1202では、図11の演算器1202と同様の演算を実行し、その出力として埋め込み済みデータx1のハッシュ値h'が出力される。こうして演算器1202からの出力である埋め込み済みデータx1のハッシュ値h'と、解析器1201から出力されたハッシュ値hとが比較器1203に入力される。そして、この比較器1203において、入力された二つのハッシュ値が等しいかどうかを比較し、その比較結果yを出力する。例えば、二つのハッシュ値が等しい場合には制御信号y="0"、二つの値が等しくない場合には制御信号y="1"を出力する。この制御信号yにより、図12の装置に入力されたデータx'が改竄されているかどうかを検証することができる。

【0101】更に、比較器1203から出力された制御信号yは、切替え器1204へ入力されても良い。この切替え器1204では、解析器1201から出力された埋め込み済みデータx1を電子透かし抽出器1205へ入力し、処理を続行するかどうかを決定する。即ち、この切替え器1204は、比較器1203から出力された制御信号yが"1"である場合には、埋め込み済みデータx1を電子透かし抽出器1205に入力させ、制御信号yが"0"である場合（一致する場合）には、埋め込み済みデータx1を電子透かし抽出器1205へ入力せずに処理を終了するように動作している。

【0102】これにより、入力されたデータが改竄されていた場合には、電子透かしの抽出を行い、入力データが改竄されていない場合には、処理を終了することが可能である。

【0103】また切替え器1204から出力された制御信号yが"1"である場合（一致しない場合）、即ち、埋め込み済み画像が改竄されていた場合には、埋め込み済み画像は電子透かし抽出器1205に入力される。電子透かし抽出器1205へ入力された埋め込み済み画像からは、乱数初期値kを用いて、埋め込まれている電子

10

20

30

40

50

透かしが出力される。この電子透かし抽出器1205の動作は、前記実施の形態1及び実施の形態2において述べた動作と同様の動作であり、改竄位置を特定することが可能なビット抽出結果画像が出力される以上述べた処理によって、入力されたデータが改竄されているかどうかを検証し、改竄されている場合には、画像上のどの箇所が改竄されていたかを特定することができる。

【0104】本発明は上記実施の形態を実現するための装置及び方法及び実施の形態で説明した方法を組み合わせて行う方法のみに限定されるものではなく、上記システム又は装置内のコンピュータ（CPUあるいはMPU）に、上記実施の形態を実現するためのソフトウェアのプログラムコードを供給し、このプログラムコードに従って上記システムあるいは装置のコンピュータが上記各種デバイスを動作させることにより上記実施の形態を実現する場合も本発明の範疇に含まれる。

【0105】またこの場合、前記ソフトウェアのプログラムコード自体が上記実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、具体的には上記プログラムコードを格納した記憶媒体は本発明の範疇に含まれる。

【0106】この様なプログラムコードを格納する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモ리카ード、ROM等を用いることができる。

【0107】また、上記コンピュータが、供給されたプログラムコードのみに従って各種デバイスを制御することにより、上記実施の形態の機能が実現される場合だけではなく、上記プログラムコードがコンピュータ上で稼働しているOS（オペレーティングシステム）、あるいは他のアプリケーションソフト等と共同して上記実施の形態が実現される場合にもかかるプログラムコードは本発明の範疇に含まれる。

【0108】更に、この供給されたプログラムコードが、コンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能格納ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって上記実施の形態が実現される場合も本発明の範疇に含まれる。

【0109】以上説明したように本実施の形態によれば、画像全体に弱く透かし情報を埋め込むことによって、改竄位置検出機能を有することを特徴とする電子透かしの埋め込み方法が可能となる。

【0110】

【発明の効果】以上説明したように本発明によれば、データに対して人為的な改竄がなされた場合に、その改竄位置を確実に検出できるという効果がある。

【0111】また本発明によれば、入力された原画像データの画素位置を指示し、主鍵情報に基づいて、その指示された画素位置の特定の部分を書き換えることにより、入力した画像データに所定のデータを埋め込むことができる。

【0112】また本発明によれば、このような所定のデータが埋め込まれたデータに対してなされた改竄処理を検知し、その改竄位置をも検知できるという効果がある。

【図面の簡単な説明】

【図1】本発明の実施の形態1に係る電子透かし埋め込み装置の概要を説明するブロック図である。

【図2】本実施の形態1に係る電子透かし抽出装置の概要を説明するブロック図である。

【図3】JPEG方式の概要を説明する図である。

【図4】JPEGによって符号化されたデータのフォーマットを説明する図である。

【図5】JPEGにおいて用いられる量子化テーブルの例を説明する図である。

【図6】JPEGにおいて用いられるジグザグスキャンを説明する図である。

【図7】JPEGにおいて用いられる交流成分のグループ分けのための例を説明する図である。

【図8】JPEGにおいて用いられる交流成分のハフマンテーブルの例を説明する図である。

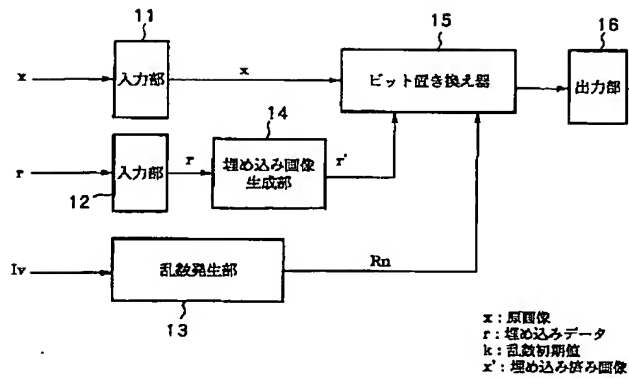
【図9】本発明の実施の形態2に係る電子透かし埋め込み装置の概要を説明するブロック図である。

【図10】本実施の形態2に係る電子透かし抽出装置の概要を説明するブロック図である。

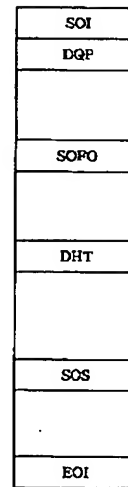
【図11】本発明の実施の形態3に係る電子透かし埋め込み装置の概要を説明するブロック図である。

【図12】本実施の形態3に係る電子透かし抽出装置の概要を説明するブロック図である。

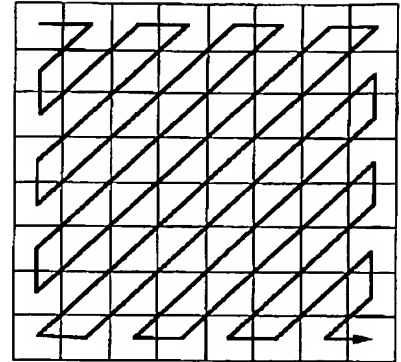
【図1】



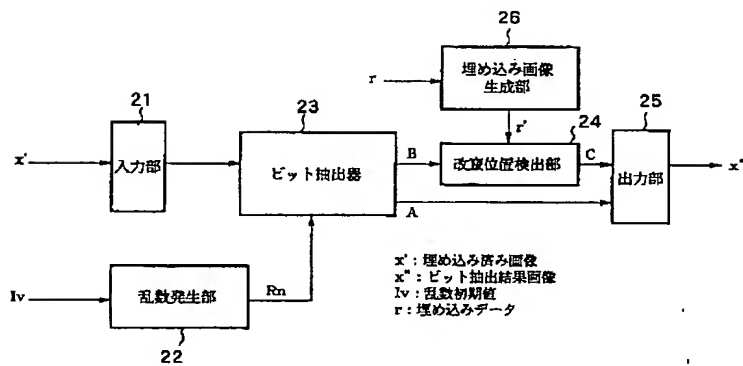
【図4】



【図6】



【図2】



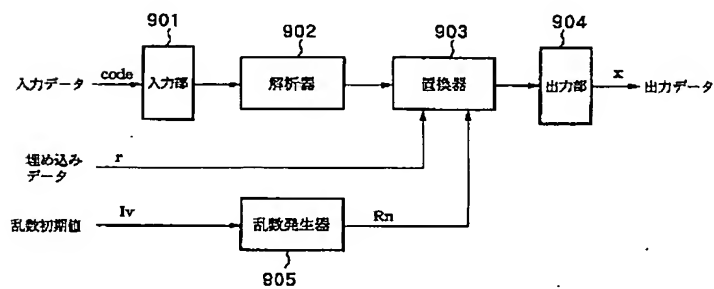
(a)

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	28	51	87	80	62
18	22	37	56	68	100	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

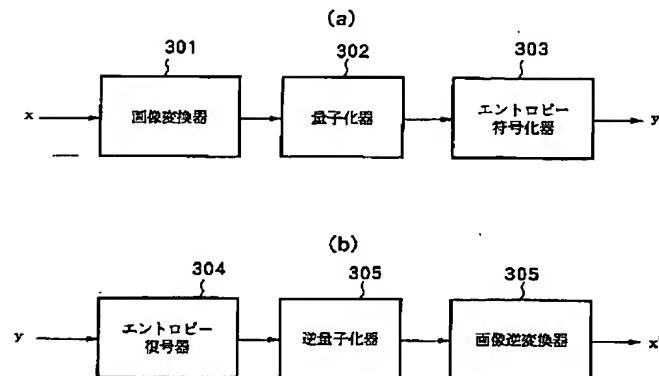
(b)

17	18	24	47	66	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
66	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

【図9】



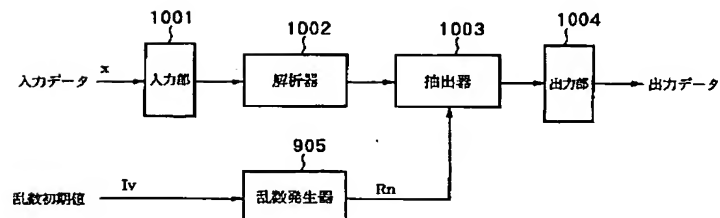
【図3】



【図7】

AC係数	グループ 番号	ランク長					
		0	1	2	...	14	15
0	0	EOB	...				
-1,1	1	00	...				
-3,-2,2,3	2	01	...				
-7,-4,4,7	3	100	...				
-15,-8,8,15	4	1011	...				
-31,-16,16,31	5	11010	...				
-63,-32,32,63	6	:					
-127,-64,64,127	7	:					
-255,-128,128,255	8	:					
以下省略							

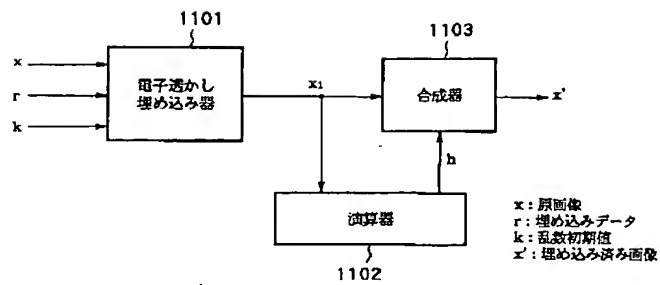
【図10】



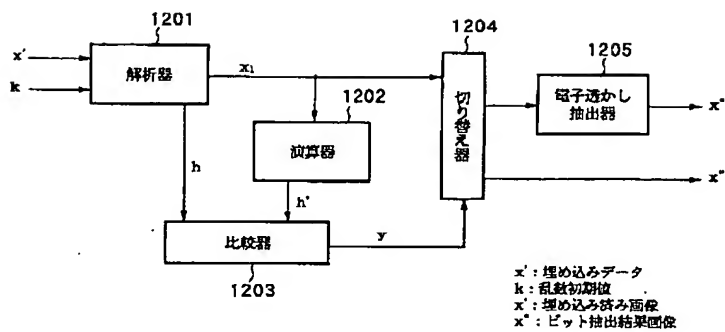
【図8】

		AC係数のグループ番号					
		0	1	2	3	...	15
零ランレングス	0	EOB	00	01	100		
	1						
	...						
	14						
	15	ZRL					

【図11】



【図12】



フロントページの続き

Fターム(参考) 5B017 AA06 BA05 BA07 BB03 CA08  
 CA09 CA16  
 5B057 CA02 CA08 CA12 CA16 CB02  
 CB06 CB08 CB12 CB16 CB19  
 CC03 CE08 CE09 CG07 CH08  
 CH20 DA07 DA17  
 5C076 AA14 AA40 BA06 CA10

(TRANSLATION)

Docket No. 5037620072

Mailing No. 033180

Mailing Date: February 3, 2004

NOTICE OF REASONS OF REJECTION

Patent Application Number:	2001-025664 for patent
Drafted Date:	January 27, 2004
Examiner:	Keigo SHIRAISHI 9856 5V00
Agent:	Hiroshi MAEDA (and other 7 persons)
Applied Law:	Sections 29(2) and 36

This application is deemed to be rejected for the following reasons. If there is any opinion thereagainst, an Argument should be filed within 60 days from the mailing date of this Notice of Reasons of Rejection.

REASONS

[A]. The inventions according to the below-mentioned Claims of this application are such as could readily be inferred, on the basis of the inventions disclosed in the publications listed below distributed prior to the filing date of this application in Japan and/or foreign countries or the inventions available to public via electric communication lines, by those who have common knowledge in the technical field to which the invention belongs. Hence, under the provision of Patent Law Section 29(2), it cannot be

patented.

REMARKS (see the below citation list about cited references.)

- Claim(s): 1 and 13
- Citation(s): 1
- Comment:

Citation 1 discloses an apparatus for embedding watermark information in image data compressed by DCT, quantization, run length encoding and Huffman coding, comprising a variable length decoding means for extracting a codeword (GC) and an additional bit or bits (VC) (definition paragraph [0057]) corresponding to the codeword from the compressed image data based on a Huffman table; an embedding means (see particularly [0072] to [0073]) for embedding watermark information in a prescribed bit of the additional bits extracted by the variable length decoding means; and a connecting means for connecting the additional bits having the watermark information embedded therein by the embedding means with the codeword extracted by the variable length decoding means to produce a variable length code.

- Claim(s): 2 and 16
- Citation(s): 1
- Comment:

Citation 1 discloses, at [0067], embedding in a high-pass component in a DCT block.

- Claim(s): 3 and 19
- Citation(s): 1
- Comment:

It is a conventional method to embed watermark information in data of which bit length is large.

- Claim(s): 4 and 22
- Citation(s): 1
- Comment:

It is a conventional method to embed watermark information in a prescribed color component.

- Claim(s): 9 to 12 and 28 to 31
- Citation(s): 1
- Comment:

To allow a header to store an area where watermark information is embedded and to extract the watermark information based on this area stored in the header are well known.

- Claim(s): 14, 17, 20 and 23
- Citation(s): 1 and 2
- Comment:

It is a well known technique to interpose electronic watermark in consideration of degradation in quality of image, as disclosed in Citation 2.

- Claim(s): 15, 18 and 21
- Citation(s): 1
- Comment:

It is a matter that a person skilled in the art naturally performs to increase the area where watermark information is to be embedded when there generates lack in this area.

#### CITATION LIST

1. JP 2001-024876A
2. JP 2000-032406A

[B] This application does not comply with the requirement under Patent Law Section 36(6)( ii ) in the following point.

#### REMARKS

(Omitted)

[C] This application does not comply with the requirement under Patent Law Section 36(6)( i ) in the following point.

#### REMARKS

(Omitted)

At the present, no reason of rejection is found for the inventions drawn to claims other than the above claims specified in the present Notice of

Reasons of Rejection. If any reason of rejection is newly found, it will be notified.

-----

Record of Result of Search for Prior Art References

• Searched Field          IPC 7th Edition    H04N 1/387

• Prior Art Reference

JP 2000-013764A

JP 2001-007705A

JP 2000-151973A

This Record of Result of Search for Prior Art References does not constitute the reasons of rejections.



整理番号:5037620072 発送番号:033180 発送日:平成16年 2月 3日 1

## 拒絶理由通知書

特許出願の番号	特願2001-025664
起案日	平成16年 1月27日
特許庁審査官	白石 圭吾 9856 5V00
特許出願人代理人	前田 弘(外 7名) 様
適用条文	第29条第2項、第36条

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から60日以内に意見書を提出して下さい。

### 理 由

[A] この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第29条第2項の規定により特許を受けることができない。

### 記 (引用文献等については引用文献等一覧参照)

- ・請求項：1, 13
- ・引用文献等：1
- ・備考：

引用文献1には、DCT・量子化・ランレングス符号化・ハフマン符号化が施されてすでに圧縮されている画像データに透かし情報を埋め込む装置であって、符号語(GC)と当該符号語に対応する付加ビット(VC) (定義段落【0057】)とをハフマンテーブルに基づいて圧縮画像データから抽出する可変長復号化手段と、前記可変長復号化手段によって抽出された付加ビットの所定のビットに透かし情報を埋め込む埋め込み手段(特に段落【0072】～【0073】を参照)と、前記埋め込み手段によって透かし情報が埋め込まれた付加ビットと前記可変長復号化手段によって抽出された符号語とを連結して可変長符号を生成する連結手段とを備える情報埋め込み装置が記載されている。

- ・請求項：2, 16
- ・引用文献等：1

・備考:

引用文献1の段落【0067】には、DCTブロックの中で、高域成分に埋め込むことが記載されている。

・請求項: 3, 19

・引用文献等: 1

・備考:

ビット長の長いデータに透かし情報を埋め込むことは常套手段である。

・請求項: 4, 22

・引用文献等: 1

・備考:

特定の色成分にのみ透かし情報を入れることは常套手段である。

・請求項: 9-12, 28-31

・引用文献等: 1

・備考:

ヘッダに透かし情報の埋め込み場所を格納すること、また、ヘッダに格納された埋め込み場所に基づいて透かし情報を取り出すことは周知技術である。

・請求項: 14, 17, 20, 23

・引用文献等: 1, 2

・備考:

引用文献2に記載されているように、画像の劣化を考慮して電子透かしを挿入することは周知技術である。

・請求項: 15, 18, 21

・引用文献等: 1

・備考:

透かし情報に対して埋め込み場所が不足した場合に埋め込み場所を増やすことは当業者が当然なし得ることである。

## 引用文献等一覧

1. 特開2001-024876号公報

2. 特開2000-032406号公報

〔B〕この出願は、特許請求の範囲の記載が下記の点で、特許法第36条第6項第2号に規定する要件を満たしていない。

記

請求項5, 7, 24, 26には、前処理として符号語の数をカウントすることが記載されているが、当該前処理が他の構成要件（本処理）とどのように関連するのかが明確でない。

〔C〕この出願は、特許請求の範囲の記載が下記の点で、特許法第36条第6項第1号に規定する要件を満たしていない。

記

請求項6, 8, 25, 27には、カウントされた符号語の数に基づいて埋め込み領域を指定する旨が記載されているが、段落【0170】では、「カウントされた符号語数および埋め込むべき透かし情報の情報量に基づいて」と記載されている。

よって、請求項6, 8, 25, 27に係る発明は、発明の詳細な説明に記載したものではない。

この拒絶理由通知書中で指摘した請求項以外の請求項に係る発明については、現時点では、拒絶の理由を発見しない。拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

-----  
先行技術文献調査結果の記録

・調査した分野 IPC第7版 H04N 1/387

・先行技術文献

特開2000-13764号公報

特開2001-7705号公報

特開2000-151973号公報

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。